SECURITY

RESPONSIBLE PROGRAM MANAGERS

Marshall Combs
Acting Director
Office of Security

Karen S. Evans
Chief Information Officer

John C. Todd
Chief
Defense Nuclear Security
National Nuclear Security Administration

DESCRIPTION OF PROBLEM

Although the Department has taken positive actions to strengthen security activities, additional improvements are needed. In addition, recent terrorist activities have prompted the Department to consider new evolving security threats and a need to identify and implement new security measures. The Department must aggressively address the challenges presented by a need for improved homeland defense, threats posed by terrorists, and the threat of weapons of mass destruction. To this end, we must develop a long-range strategic plan for the Department's security posture, conduct threat analyses to establish the framework for continually improving security protective measures, continue to implement corrective actions for cyber security, and enhance the physical security of our facilities. It is anticipated that we will have to commit significant additional resources to protect against these new evolving threats.

Further, as a result of reports by the General Accounting Office (GAO) and the Inspector General, the Department identified several areas requiring increased management attention during FY 2003 including aggressive plans of action to improve them. Security was one of these areas and the action plans to improve them are integrated within the Critical Milestones of this plan. These include: (1) Implementation plans for protection strategies in response to the new Design Basis Threat and initial resource strategy and prioritization for Design Basis Threat driven upgrades; (2) corrective action plans for Inspector General findings and General Accounting Office uncompleted security recommendations; and (3) clarification of Departmental roles and responsibilities.

PRIOR YEAR ACCOMPLISHMENTS

The Department has taken a number of actions to improve security activities. During FY 2003, we developed and published a 10-year Department-wide Strategic Plan for Security. In addition, the Department drafted a 25-year Strategic Plan that is under review. The Department also issued the new Design Basis Threat Analysis and the Annual Policy

Assessment Report. The Annual Policy Assessment Report will be refined on an annual basis, and will serve to establish the framework for continually improving security protective measures throughout the Department. In FY 2003, increased security protective measures were implemented for the Department's facilities in the National Capital Area and the Executive Protective Force was enhanced. In addition, the Department developed an initial resource strategy and prioritization for Design Basis Threat-driven upgrades. A senior management working group was established to ensure our security operations are well coordinated, facilitate our relationship with the Department of Homeland Security, and recommend actions to strengthen accountability.

The Department has addressed Inspector General (IG) recommendations on classified information systems by finalizing the appraisal process guide for documenting cyber security reviews and the technical standard operating procedure to provide guidance for conducting cyber security performance testing. The Department has implemented prior IG recommendations relating to "Virus Protection Strategies and Cyber Security Incident Reporting" by adopting and utilizing a Department virus solution application and finalization of DOE N 205.4, Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents, to clarify incident handling and reporting procedures. In addition, during FY 2002, the Department addressed the IG's recommendations on the Unclassified Cyber Security Program. Specifically, the Cyber Security Improvement Plan was developed and the Department promulgated a series of directives to support the policy document, P205.1. The directives provide the framework for a risk management approach to provide a level of protection for unclassified systems commensurate with the risk to these systems. Also in FY 2003, the CIO issued "Requirements for Cyber Security Performance Measurement Metrics" which requires quarterly reporting by Heads of Departmental Elements.

	Projected Completion Date			
PLANNED CRITICAL MILESTONES	**Previously Reported Date**	**Current Completion Date**	**Responsible Office**	**Responsible Individual**
Publish 25-Year Security Strategic Plan.	N/A	10/03	SO	Marshall Combs
Conduct Vulnerability Assessments by DOE site in accordance with the new Design Basis Threat (DBT).	N/A	10/03	SO Lead Appropriate DOE Elements	Marshall Combs and Heads of Appropriate DOE Elements
Develop Implementation Plans for near- and	N/A	10/03	SO Lead	Marshall

long-term protection strategies in response to new DBT.			Appropriate DOE Elements	Combs and Heads of Appropriate DOE Elements
Clarify Departmental security roles and responsibilities.	N/A	10/03	SO Lead and Appropriate DOE Elements	Marshall Combs Heads of Appropriate DOE Elements
Submit comprehensive corrective action and/or completion plans for IG findings and uncompleted GAO-identified security initiatives to the Deputy Secretary.	N/A	10/03	SO Lead and Appropriate DOE Elements	Marshall Combs Heads of Appropriate DOE Elements
Complete study groups on security operations and security personnel and present recommendations to the Administrator, NNSA	N/A	04/04	NNSA	John Todd
Conduct a table top exercise at the Western Area Power Administration as part of the Department's program to ensure adequate protection of internal critical infrastructures. These exercises include senior management from Federal, state and local offices who would be responsible for responding to an actual incident.	N/A	5/04	SO	Marshall Combs
Implement increased security protective measures for DOE facilities in the National Capital Area.	N/A	9/04	SO	Marshall Combs
In collaboration with other related functional needs of the Department, complete arrangements for a facility that serves the Continuity Of Operations Plan (COOP) requirements for the Department.	N/A	9/04	SO	Marshall Combs
Pursue legislation to broaden the arrest and general law enforcement authorities for DOE Special Agents.	N/A	9/04	SO	Marshall Combs
Upgrade and improve the Nuclear Materials Management and Safeguards System (NMMS),	N/A	9/04	SO	Marshall Combs

the Department's official nuclear material accounting system to result in increase accuracy and reliability of NMMSS data.				
Develop resource plans and strategies for a comprehensive review of the Department's sensitive document generation practices to improve identification of documents requiring security protection at time of origin.	N/A	9/04	SO	Marshall Combs
As part of the Department's effort to improve security of radioactive materials and in concert with the Department's acceptance of a DOE/Nuclear Regulatory Commission interagency working group recommendation to establish a national registration and tracking system for sealed sources, the Department will verify, update, and rebaseline the information contained in the existing Nonactinide Isotope and Sealed Source Database.	N/A	9/04	SO	Marshall Combs
Implement IG recommendations resulting from the IG's FY 2003 Evaluation of the Department's Unclassified Cyber Security Program.	N/A	09/04	CIO	Karen Evans
Implement approved recommendations of study groups regarding security operations and security personnel	N/A	12/05	NNSA	John Todd
Implement new Design Basis Threat throughout NNSA complex	N/A	09/06	NNSA	John Todd

PROGRESS STATUS

Although the Department has made significant progress, improving security is an iterative and evolving improvement process, especially with the renewed emphasis placed on this program as a result of the September 11, 2001, terrorist attacks. The Department has reemphasized that our overarching mission is national security. To this end, we are aggressively addressing the challenges presented by a need for improved homeland defense, threats posed by terrorists, and the threat of weapons of mass destruction. DOE's response to these threats and allocation of adequate resources to these missions will likely have far reaching consequences for the Department's budget, programs, and organization.

Additional improvements are needed to foster long-term improvement. Publication of the 25-year Strategic Security Plan will serve as the roadmap for future planning activities. With its publication, all Departmental Elements will need to develop meaningful and objective long-term security planning initiatives. Additionally, organizations will need to conduct Vulnerability Assessments for their sites in accordance with the new Design Basis Threat. Continuous process improvements via the Annual Assessment of Policy Report will assist in the continuing development of effective, clear, and comprehensive security and classification policies for DOE-wide application.

PROPOSED CLOSURE DATE

The completion of identified milestones indicate a closure date of FY 2006, however, due to continuing security challenges, we anticipate that the final correction of this issue will be a long-term effort.